PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-112937
(43)Date of publication of application : 22.04.1994

(51)Int.Cl. H04L 9/06
H04L 9/14
H04L 12/22

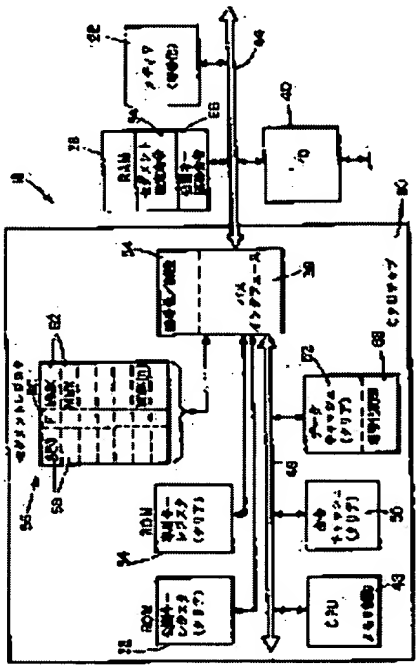
(21)Application number : 05-153959
(22)Date of filing : 24.06.1993

(30)Priority
Priority number : 92 928850 Priority date : 11.08.1992 Priority country : US

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : HARTMAN JR ROBERT C

(54) SYSTEM AND METHOD OR DATA PROCESSING

(57)Abstract:
PURPOSE: To allow the system to process both encrypted and decoded data and instructions in a seamless way.
CONSTITUTION: Internal cache memories 50, 52 are provided in safe physical areas which are not accessible by system users. An external memory 38 stores encrypted and decoded data and instructions. An interface circuit 38 decodes each encryption master key by using a private key and decodes encrypted data and instructions, corresponding to each decoded master key. A plurality of segment registers 56 stores recording of active memory segments of the external memory 38 to make them correspond to each decoded master key. A central processing unit 48 accesses both the segments of the encrypted and decoded data and instructions from the external memory 38. The encrypted information from the external memory 38 is decoded in the internal memory caches 50, 52, and non-encrypted information is stored directly.



LEGAL STATUS

[Date of request for examination] 24.06.1993
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2085066

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－112937

(43)公開日　平成６年(1994)４月22日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/06					
9/14					
12/22					
		7117－5K	Ｈ０４Ｌ	9/ 02	Ｚ
		8732－5K		11/ 26	

審査請求　有　　請求項の数８（全　９　頁）

(21)出願番号　特願平5－153959

(22)出願日　平成５年(1993)６月24日

(31)優先権主張番号　９２８８５０

(32)優先日　1992年８月11日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州アーモンク　（番地なし）

(72)発明者　ロバート　チャールズ　ハートマン、ジュニア
アメリカ合衆国94062－0717、カリフォルニア州ウッドサイド、ピー．オー．ボックス　620717

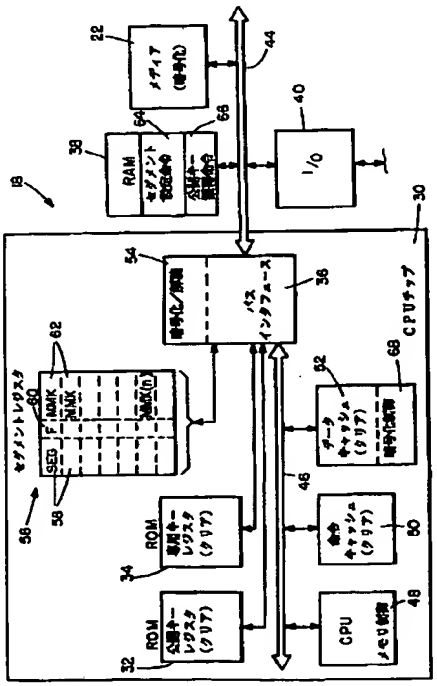
(74)代理人　弁理士　合田　潔　（外４名）

(54)【発明の名称】　データ処理システム及び方法

(57)【要約】

【目的】　暗号化及び非暗号化データ及び命令の両方をシームレスに処理する。

【構成】　データ処理システムは、システムユーザへアクセス不能な安全物理領域に内部キャッシュメモリ５０、５２を有する。外部メモリ３８は、暗号化及び非暗号化データ及び命令を記憶する。インタフェース回路３６は、専用キーの使用により各暗号化マスタキーを解読すると共に、解読された各マスタキーに対応する暗号化データ及び命令を解読する。複数のセグメントレジスタ５６は、外部メモリ３８のアクティブメモリセグメントの記録を保持し、それと解読された各マスタキーとを対応させる。中央処理装置４８は外部メモリ３８からの非暗号化及び暗号化データ及び命令の両方のセグメントをアクセスする。外部メモリ３８からの暗号化情報は解読されて内部メモリキャッシュ５０、５２に記憶され、非暗号化情報は直接記憶される。



1

【 特許請求の範囲】

【 請求項1 】　暗号化及び非暗号化データ及び命令の両方を処理するためのデータ処理システムであって、前記システムのユーザへアクセス不能な安全物理領域を含み、

暗号解読されたディジタル情報及び非暗号化ディジタル情報を記憶するための、前記安全物理領域内の内部メモリ手段と、

暗号化マスタキーを解読する際に使用するため前記安全物理領域内の専用キーをアクセスするとの命令を記憶するための、前記安全物理領域外側の外部メモリ手段と、

アクセスされた専用キーの使用により前記暗号化マスタキーを解読すると共に前記マスタキーで暗号化された情報を解読するための、前記安全物理領域内のインタフェース手段と、

アクティブメモリセグメントの記録を保持すると共に、解読されたマスタキーをそれと対応させるための、前記安全物理領域内のセグメントレジスタ手段と、

前記外部メモリ手段のアドレスに記憶された非暗号化及び暗号化情報の両方のセグメントをアクセスすると共に、アクセスされたアドレスと前記セグメントレジスタ手段内で対応される前記解読されたマスタキーを前記インタフェース手段に使用させて、前記アドレスからの情報を解読し、解読された情報を前記内部メモリ手段に記憶し、前記外部メモリ手段からの情報が暗号化されていない場合には前記情報を前記内部メモリ手段に直接記憶するための、前記安全物理領域内の中央プロセッサと、を備えたデータ処理システム。

【 請求項2 】　前記情報はデータ又は命令のどちらか、もしくは両方である請求項1 記載のデータ処理システム。

【 請求項3 】　前記セグメントレジスタ手段は複数のレジスタを備え、前記レジスタのそれぞれは、セグメントアドレス及び長さ又はエンドアドレスフィールドと、フラッグフィールドと、解読されたメディアマスタキーを保持するためのフィールドと、を有し、前記レジスタのそれぞれは前記セグメント内のデータアドレスのアクセスの際に前記ＣＰＵにより使用される請求項1 記載のデータ処理システム。

【 請求項4 】　前記中央プロセッサ及び前記インタフェース手段間で転送される全ての命令及びデータは、前記安全物理領域内で発生し、これによりユーザへアクセス不能である請求項1 記載のデータ処理システム。

【 請求項5 】　前記セグメントレジスタ手段は前記メディアマスタキーの使用により暗号化されたメディアに格納されるデータ及び命令を解読するために複数の解読されたメディアマスタキーを記憶し、前記解読されたデータ及び命令は前記中央プロセッサにより使用される請求項1 記載のデータ処理システム。

【 請求項6 】　暗号化及び非暗号化データ及び命令の両

2

方を処理するデータ処理システムにおけるデータ処理方法であって、前記システムは前記システムのユーザへアクセス不能な安全物理領域を含み、

前記安全物理領域に暗号解読されたディジタル情報及び非暗号化ディジタル情報を記憶するステップと、

前記安全物理領域の外側の外部メモリ手段に、暗号化マスタキーを解読する際に使用するため前記安全物理領域内で専用キーをアクセスするとの命令を記憶するステップと、

前記安全物理領域内のインタフェース手段においてアクセスされた専用キーの使用により前記暗号化マスタキーを解読すると共に、前記マスタキーで暗号化された情報を解読するステップと、

前記安全物理領域内のセグメントレジスタ手段に、アクティブメモリセグメントの記録と対応する解読されたマスタキーとを保持するステップと、

前記安全物理領域内で、前記外部メモリ手段のアドレスに記憶された非暗号化及び暗号化情報の両方のセグメントをアクセスするステップと、

アクセスされたアドレスと前記セグメントレジスタ手段で対応される前記解読されたマスタキーを前記インタフェース手段に使用させ、前記アドレスからの情報を解読するステップと、

前記解読された情報を前記内部メモリ手段に記憶し、前記外部メモリ手段からの情報が暗号化されてない場合には前記情報を前記内部メモリ手段に記憶するステップと、

を含むデータ処理方法。

【 請求項7 】　前記セグメントレジスタ手段は、前記データセグメント内の情報が暗号化されているか否かを示すフラッグを含み、前記インタフェース手段は、前記外部手段からの情報の処理において前記フラッグに応答する請求項6 記載のデータ処理方法。

【 請求項8 】　暗号化情報を含むメモリセグメントを非暗号化命令がアクセスすることを防止するステップを更に含む請求項6 記載のデータ処理方法。

【 発明の詳細な説明】

【 ０００１ 】

【 産業上の利用分野】本発明は、暗号化及び非暗号化データ及び命令をシームレス(seamless) 処理するためのシステムに関し、更に詳細には、暗号化メディアの不正使用を防止する暗号構造機能を組み込むデータ処理システムに関する。

【 ０００２ 】

【 従来の技術】実質的な努力は専売ソフトウェアのコピー防止に対して行われてきた。このような努力は一般的に失敗に終わり、現在では、専売ソフトウェアを保護するための最も有効な方法は使用保護手段によるものであり、コピーの保護ではないことが認められている。使用保護は、一般的に、ソフトウェアの暗号化及び使用時に

3

おけるその暗号解読を含む。提供者及び消費者間でディジタル情報を安全に送信するために使用される伝統的な方法は、米国標準局により「 データ暗号化標準(Data Encryption Standard) 」に規定されているような単一キー暗号システムによるものである。このプロセスでは、単一キーは暗号化及び暗号解読のために使用され、秘密に保持され、更に機密保護のため頻繁に変更される。キー変更のための1 つのプロセスは「 キー連鎖(key chaining) 」と呼ばれ、暗号化データストリーム内の合意された位置に新しいキーを配置することを含む。この方法の絶対的な機密保護は、少なくとも、１つのシードキー(seed key) の機密性に頼っている。通常、データ通信チャネルは物理的に安全ではないので、シードキーは、信頼されている伝達手段(courier) 等の物理的に安全なチャネルを介して消費者へ伝達されることが多い。これは、多数の消費者及び多数のデータストリーム型を有する高ボリューム環境のためには実際的な方法ではない。

【０００３】公開及び専用キーを使用する二重キー暗号システムは、キー分配の問題を排除することができるが、データストリームが消費者独自の公開キーで暗号化されることを必要とする。このような例では、「 公開キー(public key) 」という用語は、その本質がメディア提供者へ公開されていることを意味する。「 専用キー(private key) 」という用語は、その本質はメディア提供者から隠されているが、もし消費者がその機密性を保持するために十分な努力を行わなければ発見され得ることを意味する。公開及び専用キーは、真の二重キー暗号システムのように、一対のキーであってもよい。あるいは、提供者及び消費者間に信頼レベルが存在すると仮定すると、専用キーは単一キー暗号システムの秘密キーであり、公開キーは実際のキーを公開することなくどの秘密キーが使用されるかを識別するために使用されてもよい。従って、全ての消費者のあるサブセットへのアクセスを制限し、二重キー暗号システムをなおも使用するために、メディア提供者は異なるように符号化されたデータストリームを各消費者へ送らなければならない。このデータストリームは次に、消費者の専用キーにより暗号解読される。この手順もまた、高ボリューム環境のためには実際的ではない。

【０００４】二重キー及び単一キー暗号システムを組み合わせると、上記の問題を低減することができる。ここでは、メディアは、提供者の物理的に安全な環境の中で、単一マスタキーにより暗号化される。マスタキー(以下、メディアマスタキー又はMMKと称する) は、次に、消費者により提供される公開キー又は提供者及び消費者の双方により所有される秘密キーを用いて更に暗号化される。次に暗号化MMKは、メディアと共に、又は別のキー要求トランザクションを介して分配される。そして消費者はその専用キーを使用して、MMKを解読

4

する。解読されたMMKは、消費者の安全な物理環境におけるメディアの暗号解読を可能にする。

【０００５】上記のデータ機密保護技法及びその変形例は、以下の先行技術に見られる。米国特許第4 、４６５、９０１号では、暗号マイクロプロセッサは、必要とする場合に暗号化命令を断片的に解読することより暗号化プログラムを実行する。プログラムの小部分を必要とされる場合にだけ暗号解読することにより、プログラム全体をその暗号が解読された形態で記憶する必要性が回避される。種々の暗号化方法が記載されており、マイクロプロセッサチップは、プログラムが1 つのチップで実行され他のマイクロプロセッサでは実行されないように、プログラム命令を暗号解読するために独自の暗号キー又はテーブルを使用できると示されている。

【０００６】米国特許第4 、５５８、１７６号では、メディア保護は、各顧客毎にメディアを独自に暗号化することによって実行される。更に、この特許の中央処理装置は、暗号化ソフトウェアから非暗号化ソフトウェアへ変わる場合にモードの切換えを要求される。従って、モード切換えを可能にするために明示された命令が提供されなければならず、アプリケーションプログラマはモード切換え要求を知っていなければならない。

【０００７】米国特許第4 、６３４、８０７号は、データ暗号化アルゴリズムを使用するホストコンピュータ及び公開／専用キーシステムの公開キーを用いて暗号化されるキーへの補足を記載している。暗号化ソフトウェアモジュールは、専用キーがデータ暗号化キーを復号するソフトウェア保護装置へ入れられる。暗号解読が一旦完了されると、ホストコンピュータは復号化ソフトウェアを使用できるようになるが、これは、ユーザへアクセス可能であり暗号解読攻撃が向けられるポイントである入力／出力チャネルを介して行うことができる。

【０００８】米国特許第4 、８０７、２８８号は、公開／専用キー暗号化機能を実行するための1 チップマイクロプロセッサについて記載している。チップマイクロプロセッサはデータを実行せず、単にデコーダとして作用する。従って、システムはマイクロプロセッサへの入力／出力ポートで攻撃を受ける。

【０００９】米国特許第4 、８５０、０１７号は、制御値が認証されており暗号キーへのアクセスを制御する二重キー暗号化システムについて記載している。

【００１０】米国特許第4 、８４７、９０２号は、複数のキーのうちの1 つを使用してメインメモリからの命令を選択的に暗号解読するコンピュータについて記載している。これらの命令がメインメモリからコンピュータに関連するキャッシュメモリへ転送される場合、命令は実行中だけ暗号解読される。この特許のシステムでは、一度にただ1 つのキーが起動され、キーの切換えはサブルーチンへの呼び出しを必要とする。従って、キーの切換えは可能であるが、これは、アプリケーションプログラ

5

マに知られており、プログラム中で説明されなければならない方法で達成される。更に、この特許には、暗号化データ及び命令の両方がアドレス指定されるとは示されていない。

【００１１】米国特許第4、８８８、７９８号は、公認要素及び非公認要素の双方を含むコンピュータソフトウェアについて記載している。ユーザは、対応する暗号化キー（通常は各公認要素に対するキー）を入力することにより１つ又はそれ以上の公認要素のロックを解除することができる。更に、多重キーは、暗号解読キーへのアクセスを可能にするために利用されると示されている。

【００１２】要約すると、先行技術は、暗号化データ及び暗号化命令の使用、ソフトウェアを暗号解読するための暗号化キーの使用、暗号解読のためのクリアキーの使用、並びに解読されたデータが保護される安全な処理環境の使用を示している。しかしながら、上記先行技術の多くでは、ユーザアクセスは、プロセッサ及び暗号解読プロセッサ間で受け渡される際にデータをクリアする又は命令をクリアするようになっている。更に、既知の先行技術では、動作プロセッサは、暗号化及び非暗号化ソフトウェアメディアを扱う場合に異なるモードで作動する必要がある。その結果、アプリケーションソフトウェア設計者はこのようなモードを常に知っていて、適切なときに実施しなければならない。

【００１３】

【発明が解決しようとする課題】従って、本発明の目的は、システムの中央処理装置が暗号化及び非暗号化データ及び命令の両方をシームレスに取り扱うことのできる、暗号化メディアを取り扱うためのシステムを提供することである。

【００１４】本発明のもう１つの目的は、中央処理装置のメモリ管理機構に一体化されるソフトウェアメディアの暗号化及び暗号解読のためのシステムを提供することである。

【００１５】更に、本発明のもう１つの目的は、明示的モード切換え命令を必要とせずに中央処理装置が暗号化及び非暗号化命令及びデータを同時にアクセスできるようにすることである。

【００１６】

【課題を解決するための手段】上記目的を達成するために、本発明の第1の態様は、暗号化及び非暗号化データ及び命令の両方を処理するためのデータ処理システムであって、前記システムのユーザへアクセス不能な安全物理領域を含み、暗号解読されたディジタル情報及び非暗号化ディジタル情報を記憶するための前記安全物理領域内の内部メモリ手段と、暗号化マスタキーを解読する際に使用するため前記安全物理領域内の専用キーをアクセスするとの命令を記憶するための前記安全物理領域外側の外部メモリ手段と、アクセスされた専用キーの使用により前記暗号化マスタキーを解読すると共に前記マスタキーで暗号化された情報を解読するための前記安全物理領域内のインタフェース手段と、アクティブメモリセグメントの記録を保持すると共に解読されたマスタキーをそれと対応させるための前記安全物理領域内のセグメントレジスタ手段と、前記外部メモリ手段のアドレスに記憶された非暗号化及び暗号化情報の両方のセグメントをアクセスすると共に、アクセスされたアドレスと前記セグメントレジスタ手段内で対応される前記解読されたマスタキーを前記インタフェース手段に使用させて、前記アドレスからの情報を解読し、解読された情報を前記内部メモリ手段に記憶し、前記外部メモリ手段からの情報が暗号化されていない場合には前記情報を前記内部メモリ手段に直接記憶するための前記安全物理領域内の中央プロセッサと、を備える。

【００１７】また本発明の第2の態様は、暗号化及び非暗号化データ及び命令の両方を処理するデータ処理システムにおけるデータ処理方法であって、前記システムは前記システムのユーザへアクセス不能な安全物理領域を含み、前記データ処理方法は、前記安全物理領域に暗号解読されたディジタル情報及び非暗号化ディジタル情報を記憶するステップと、前記安全物理領域の外側の外部メモリ手段に、暗号化マスタキーを解読する際に使用するため前記安全物理領域内で専用キーをアクセスするとの命令を記憶するステップと、前記安全物理領域内のインタフェース手段においてアクセスされた専用キーの使用により前記暗号化マスタキーを解読すると共に、前記マスタキーで暗号化された情報を解読するステップと、前記安全物理領域内のセグメントレジスタ手段に、アクティブメモリセグメントの記録と対応する解読されたマスタキーとを保持するステップと、前記安全物理領域内で、前記外部メモリ手段のアドレスに記憶された非暗号化及び暗号化情報の両方のセグメントをアクセスするステップと、アクセスされたアドレスと前記セグメントレジスタ手段で対応される前記解読されたマスタキーを前記インタフェース手段に使用させ、前記アドレスからの情報を解読するステップと、前記解読された情報を前記内部メモリ手段に記憶し、前記外部メモリ手段からの情報が暗号化されてない場合には前記情報を前記内部メモリ手段に記憶するステップと、を含む。

【００１８】

【作用】データ処理システムは、ここでは、暗号化及び非暗号化データ及び命令の両方をシームレス処理する。システムは、システムのユーザへアクセス不能な安全物理領域（secure physical region）に内部キャッシュメモリを有する。外部メモリは安全物理領域の外側に配置され、暗号化及び非暗号化データ及び命令を記憶する。システムは、安全物理領域内に含まれる専用キーをアクセスするとの命令を有する。このキーは、暗号化データ及び命令を伴う暗号化マスタキーを解読するために使用される。インタフェース回路は安全物理領域に配置さ

6

7

れ、専用キーの使用により各暗号化マスタキーを解読すると共に、解読された各マスタキーに関連する暗号化データ及び命令を解読する。安全物理領域の複数のセグメントレジスタは外部メモリ内のアクティブメモリセグメントの記録を保持し、それと解読された各マスタキーとを対応させる。中央処理装置は外部メモリからの非暗号化及び暗号化データ及び命令の両方のセグメントをアクセスし、これによりインタフェース回路は、解読されたマスタキーを使用して外部メモリからのデータ及び命令を解読するとともに、解読された情報を内部メモリキャッシュに記憶する。非暗号化データ及び命令は内部メモリキャッシュに直接記憶される。

【００１９】

【実施例】図1において、メディア提供者（プロバイダ）１０は、公開キー１２及び専用キー１４の対応する対の安全記憶に対して責任のある機能である。公開キー１２は、製造者又はメディア提供者１０により割り当てられる遠隔プロセッサのシリアル番号又は他の番号である。専用キー１４は、メディア提供者１０又は遠隔プロセッサの売主あるいは他のソースにより遠隔プロセッサへ割り当てられる番号又は他の英数字シーケンスである。公開及び専用キー１２及び１４は、真の二重キー暗号システムにおけるような一対のキーであってもよい。あるいは、専用キー１４は単一キー暗号システムの秘密キーであり、公開キー１２はどの秘密キーが使用されるかを実際のキーを公開することなく識別するための手段として使用されてもよい。メディア提供者１０は、全ての公開キー１２及びその対応の専用キー１４の完全な記録を含む。また、メディア提供者１０は、メディア１７を暗号化するために使用されるMMK１６と、暗号化メディアを識別する対応のメディア識別子と、を含む。

【００２０】遠隔プロセッサ１８は、二重通信チャネル２０を介してメディア提供者１０へ接続される。遠隔プロセッサ１８は暗号化メディア２２のための入力を有し、その公開及び専用キーの両方のコピーを記憶装置に格納する。このような記憶装置はユーザへ物理的にアクセス不能である。公開キーはプログラム命令を介してユーザへアクセス可能である。遠隔プロセッサ１８は、メディア提供者１０から直接チャネル２０を介して、又はローカルソースから、暗号化メディアを得ることができる。いずれの場合でも、メディアは、メディアマスタキーを用いて一般に暗号化される。異なるメディアは、異なるメディアマスタキーで暗号化されることができる。

【００２１】一旦ユーザが暗号化メディア２２を得ると、直接又はチャネル２０を介して、ユーザは遠隔プロセッサ１８にメディアキー要求をメディア提供者１０へ伝送させる。メディアキー要求には、ユーザの公開キーのコピー及び要求されたメディアのメディア識別子が含まれる。その情報がメディア提供者１０により受信されると、受信された公開キー１２は局部的に記憶された

8

（対応する）専用キー１４がアクセスされるのを可能にする。同時に、メディア識別子は、要求されたメディアを暗号化するために使用された特定のメディアマスタキーをアクセスするために使用される。そして、アクセスされた専用キー１４はメディアマスタキーを暗号化するために使用され、暗号化されたメディアマスタキーは、メディア提供者１０からのメディアキー応答の一部として遠隔プロセッサ１８へ戻すよう伝送される。

【００２２】暗号化メディアマスタキーが受信されると、それは遠隔プロセッサ１８の安全物理領域内へ入力され、そこに記憶される専用キー１４のコピーを用いて解読される。次に、メディアマスタキーのクリアコピーは安全物理領域内に記憶され、遠隔プロセッサ１８の安全物理領域内で処理される際にメディアを暗号解読するために使用される。

【００２３】上記のようにして、公衆に対してアクセス可能な任意の機能において専用キー１４又はメディアマスタキーの解読されたコピーを公開しないことにより、安全性は保持される。更に、暗号化メディアは解読され、利用され、そしてもし必要なら、再度暗号化されるが、これらは全て、遠隔プロセッサ１８内の安全物理領域内で行われる。このようにして、暗号化メディア２２の使用は制御され、特別に暗号化されるのはメディアマスタキーだけであり、メディアの個別的暗号化の必要はない。従って、メディアマスタキーの暗号化状態が安全に保持される限りは、暗号化メディア２２は一般に分配されることができる。暗号化メディアは、適切に符号化されたメディアマスタキーが提供されなかったものには使用不能である。

【００２４】次に図2を参照すると、プロセッサ１８内の安全物理領域は、ＣＰＵ半導体チップ３０及びそれに含まれる回路を含む。これらはすべて、ユーザにアクセス不能である。以下の説明から理解されるように、ＣＰＵチップ３０内でのみ、クリア形態の解読されたメディア、専用キー１４のクリアコピー、及び種々のメディアマスタキーの解読されたコピーが見られる。

【００２５】ＣＰＵチップ３０は2つのプログラマブル読取専用メモリ（ＲＯＭ）レジスタを含み、１つのレジスタ３２は解読された形の公開キー１２を含み、１つのレジスタ３４は解読された形のプロセッサ専用キー１４を含むためのものである。両レジスタとも、製造者又は第1販売者によりプログラミングされ、一旦プログラミングされると変更されない。上記のように、公開キーレジスタ３２の値は製造者により割り当てられるプロセッサ１８のシリアル番号でもよい。専用キーレジスタ３４の番号は製造者により割り当てられる識別子であり、プロセッサ１８内で公開キーレジスタ３２と独特に対とされる。

【００２６】レジスタ３２及び３４は、その出力を、ＣＰＵチップ３０とプロセッサ１８の外部構成要素との間

の全てのインタフェース機能を提供するバスインタフェースモジュール３６へ提供する。これらの外部構成要素には、ランダムアクセスメモリ（ＲＡＭ）３８、１つ又はそれ以上のI／Oポート４０、及び1つ又はそれ以上のメディアシステム２２が含まれる。メディアシステム２２は、フロッピーディスクシステム、カートリッジ読取専用又は読取／書込システム等である。プロセッサ１８の上述の構成要素のそれぞれは、バス４４を介してバスインタフェースモジュール３６へ接続される。

【００２７】ＣＰＵチップ３０内において、バス４６は、ＣＰＵ４８、命令キャッシュ５０、及びデータキャッシュ５２間の内部通信を提供する。バスインタフェース３６内には、ＣＰＵチップ３０内で使用するためにバス４４で入力される暗号化命令及びデータを解読し、ＲＡＭ３８に記憶してI／Oポート４０又はメディア２２へ渡すためにバス４４で出力されるデータを暗号化する機能を果たす暗号化／解読モジュール５４が含まれる。バス４４もしくはモジュール３８、４０又は２２には、「安全な」データは解読された状態では現れない。

【００２８】複数のメモリセグメントレジスタ５６はバスインタフェース３６へ接続され、既知のセグメント識別機能の提供に加えて、メモリセグメント内の情報が暗号化情報を含むか否か、もし含むなら、暗号化情報を解読する解読されたメディアマスタキーを含むか否かを示す特別機能を実行する。当業者には知られているように、セグメントレジスタはメモリのどの部分をプログラムが使用するかを制御する値を保持し、コードセグメント、データセグメント又はスタックセグメントとして分類される。

【００２９】ＣＰＵチップ３０はセグメント化メモリを有し、プログラムへのメモリのアドレス空間はチャンク（chunk）又はセグメントへ分割され、プログラムはこれらのセグメントに含まれるデータをアクセスできるだけである。各セグメント内では、アドレス指定は線形であり、プログラムはバイト０、バイト１、バイト２等をアクセスすることができ、アドレス指定はセグメントの開始に関連している。アクティブデータ／命令セグメントは、セグメントレジスタ５６の様々なもののプログラム使用により追跡される。

【００３０】各セグメントレジスタ５６は、セグメントの開始アドレスと、長さ指名子又はセグメントに含まれるデータ／命令の最終アドレスと、を含む第1フィールド５８を含む。

【００３１】メモリセグメントが暗号化されているか暗号化されていないかの表示を含む追加のセクション６０はフィールド５８に対応している。フィールド６０は単一ビット（又はフラッグ）から成り、このような表示を提供する。また、各セグメントレジスタは、対応のメモリセグメントに記憶される情報の解読を可能にする解読されたメディアマスタキーを記憶するための第3フィールド６２を有する。

【００３２】異なるソースからの種々のプログラムセグメントがＣＰＵチップ３０の動作中に実施されるので、複数のセグメントレジスタ５６が提供され、その暗号化状態と、メモリセグメント内の情報の解読又は暗号化に使用されるメディアマスタキーと、を示すためにそれぞれ別々にプログラミングされる。

【００３３】上記に示したように、本発明の目的は、プロセッサ１８のメモリ管理機構に一体化されるように暗号化及び暗号解読を達成することである。このようにプロセッサ１８内の手順を編成することにより、保護（暗号化）された命令及びデータは保護されていない命令及びデータと共にアクセスされることができ、プロセッサ内の明示的モード切換えの必要がない。すなわち、プロセッサ１８内の手順は、データ／命令が暗号化されているかいないかに対して透過的なモードで作動する。この動作方法は、プロセッサ１８のオペレーティングシステムにより使用される２つの特別な命令を含むことによって達成される。これらの命令は、セグメントキー設定（Set Segment Key）命令６４及び公開キー獲得（Get Public Key）命令６６としてＲＡＭ３８に概略的に示される。

【００３４】セグメントキー設定命令６４は、専用キーレジスタ３４（ＣＰＵチップ３０内）の専用キー値１４を使用して、受信した暗号化メディアマスタキーを解読する。得られたクリアメディアマスタキーは、特別なメディアマスタキーで暗号化された特定のプログラムセグメントに隣接する位置６２においてセグメントレジスタ５６に記憶される。また、セグメントキー設定命令６４は、対応の暗号化ビット６０をオン又はオフするためにも使用される。理解されるように、セグメントキー設定命令６４はＲＡＭ３８に常駐するが、そのコマンドに従って実行される全ての機能はＣＰＵチップ３０内で発生し、ユーザからは隠されている。

【００３５】公開キー獲得命令６６は、公開キーレジスタ３２から公開キー値１２を戻す。上述のように、公開キーレジスタ３２の公開キー値はＣＰＵチップ３０に独特の番号であり、メディア提供者１０（図1）では、専用キーレジスタ３４の専用キー値１４と対応している。メディア提供者１０内では、プロセッサ１８から受信される公開キー値１２は、記憶され対応されるプロセッサ１８の専用キー値１４をアクセスするために使用される。次に、その専用キー値は、メディア２２を暗号化するために使用されたメディアマスタキーを暗号化するために使用される。

【００３６】メディア提供者１０が暗号化メディアマスタキーをメディア４２又はI／Oポート４０を介してプロセッサ１８へ戻す際、それは一時的にＲＡＭ３８に記憶される。次に、セグメントキー設定命令６４が実行され、暗号化メディアマスタキーは、バスインタフェース

11

３６へ読み出される。バスインタフェース３６は、暗号化／解読モジュール５４の制御の下、専用キー値１４（専用キーレジスタ３４に記憶される）を使用し、専用キー１４を用いてメディアマスタキーを解読する。解読されたメディアマスタキーは、次に、メディアマスタキーで暗号化されたメディアのアドレスに隣接するフィールド６２においてセグメントレジスタ５６に配置される。同時に、対応するレジスタ位置６０のビットが設定され、セグメントが暗号化されたことを表示する。

【００３７】ここで、ＣＰＵ４８が命令キャッシュ５０又はデータキャッシュ５２のいずれにも存在しないデータ又は命令を呼び出すと仮定すると、このような命令によって、情報が暗号化されようとされまいと、適切な情報がＲＡＭ３８からバスインタフェース３６へ読み出される。情報が暗号化されると、バスインタフェース３６は、メモリセグメントフィールド６０のフラッグの状態によりその事実を知る。データセグメントが暗号化されるとすると、バスインタフェース３６は、リコールされたアドレスに対応するセグメントレジスタ５６のフィールド６２の解読されたメディアマスタキーを呼び出す。次に、そのメディアマスタキーは入力情報を解読するために暗号化／解読モジュール５４により使用され、解読された情報は、場合次第でデータキャッシュ５２又は命令キャッシュ５０のいずれかに配置される。

【００３８】対照してみると、バスインタフェース３６がＲＡＭ３８から非暗号化データを受信すると、対応のセグメントレジスタ５６のフィールド６０に設定フラッグがないことにより、到着情報が暗号化されていないことが示される。このような場合、バスインタフェース３６は、要求されたデータを変更することなくそれぞれのキャッシュメモリへ渡す。

【００３９】従ってわかるように、ＣＰＵチップ３０は、データが暗号化されるか否か、又は多数のメモリセグメントのうちのどれがデータを格納するかにかかわらず、データ上でシームレスに作動する。暗号化データを取り扱うためにモード切換えは必要でなく、解読されたデータ／命令はユーザには使用不能である。システムが２つ以上のＣＰＵチップを必要とする場合、バスインタフェースは、暗号化データのみがチップ間を移動するように各ＣＰＵチップ毎に提供されなければならない。

【００４０】データの更なる機密保護を可能にするために、暗号化制御モジュール６８はデータキャッシュ５２内に含まれ、暗号化データセグメントが暗号化命令セグメント以外から参照されるのを防止する。従って、実行命令がデータキャッシュ５２からデータを参照する場合、暗号化制御６８は、セグメントレジスタ５６のフィールド６０に設定フラッグを含むメモリセグメント内に命令が常駐するかどうかを決定するために検査する。フィールド６０のフラッグが設定されていると、命令は、そのデータ／命令が暗号化又は非暗号化メモリセグメントからのものであるかにかかわらずデータ又は命令を呼び出すことが可能になる。命令が非暗号化コードセグメントからであると示されると、暗号化制御６８はそれが暗号化データセグメントを参照するのを防止する。この機能は、分解によるコードのリバースエンジニアリングを防止する。また、侵入者が暗号化データセグメントを非暗号化データセグメントにコピーするためにプログラムを作成するのを防止する。これは、メディア提供者だけがプログラムのための暗号化MMKを作成することができるので、全ての暗号化プログラム命令はメディア提供者からのものでなければならないからである。

12

【００４１】最後に、セグメントレジスタ５６が仮想メモリプロセッサシステムで使用される場合には、セグメントキー設定命令は、暗号化メディアマスタキー及びフラッグのためのフィールドを追加して現存の仮想セグメント記述子を拡張することにより間接的に実行される。これらのフィールドは、対応の仮想メモリセグメントの暗号化／非暗号化状態を示す。

【００４２】

【発明の効果】以上説明したように、本発明のデータ処理システムによって、暗号化及び非暗号化データ及び命令の両方をシームレスに取り扱うことができるという優れた効果が得られる。

【図面の簡単な説明】

【図１】メディア提供者及び遠隔プロセッサ間の相互作用を示し、これにより、暗号化メディアは暗号化メディアマスタキーと共に遠隔プロセッサへ転送される。

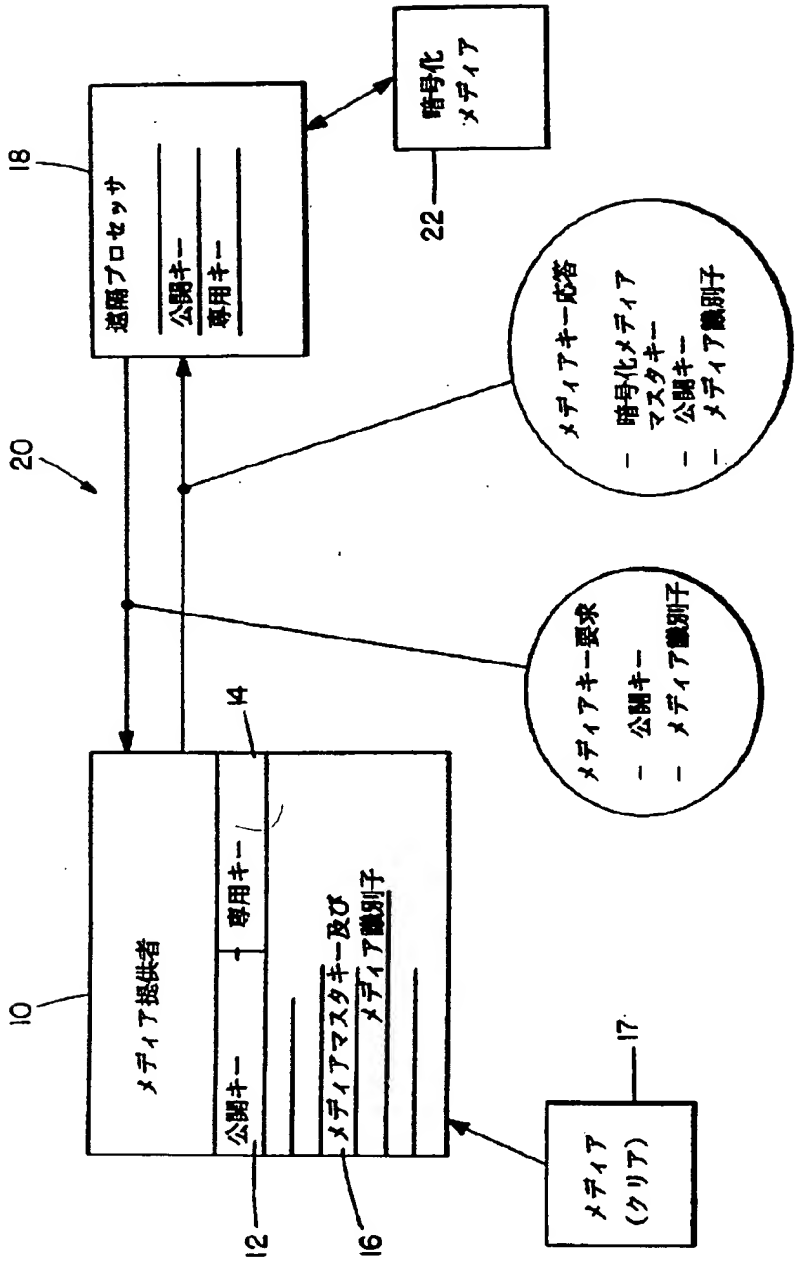
【図２】図1の遠隔プロセッサの一部のブロック図であり、メディアマスタキー及び受信情報の暗号化／暗号解読に含まれる部分を説明する。

【符号の説明】

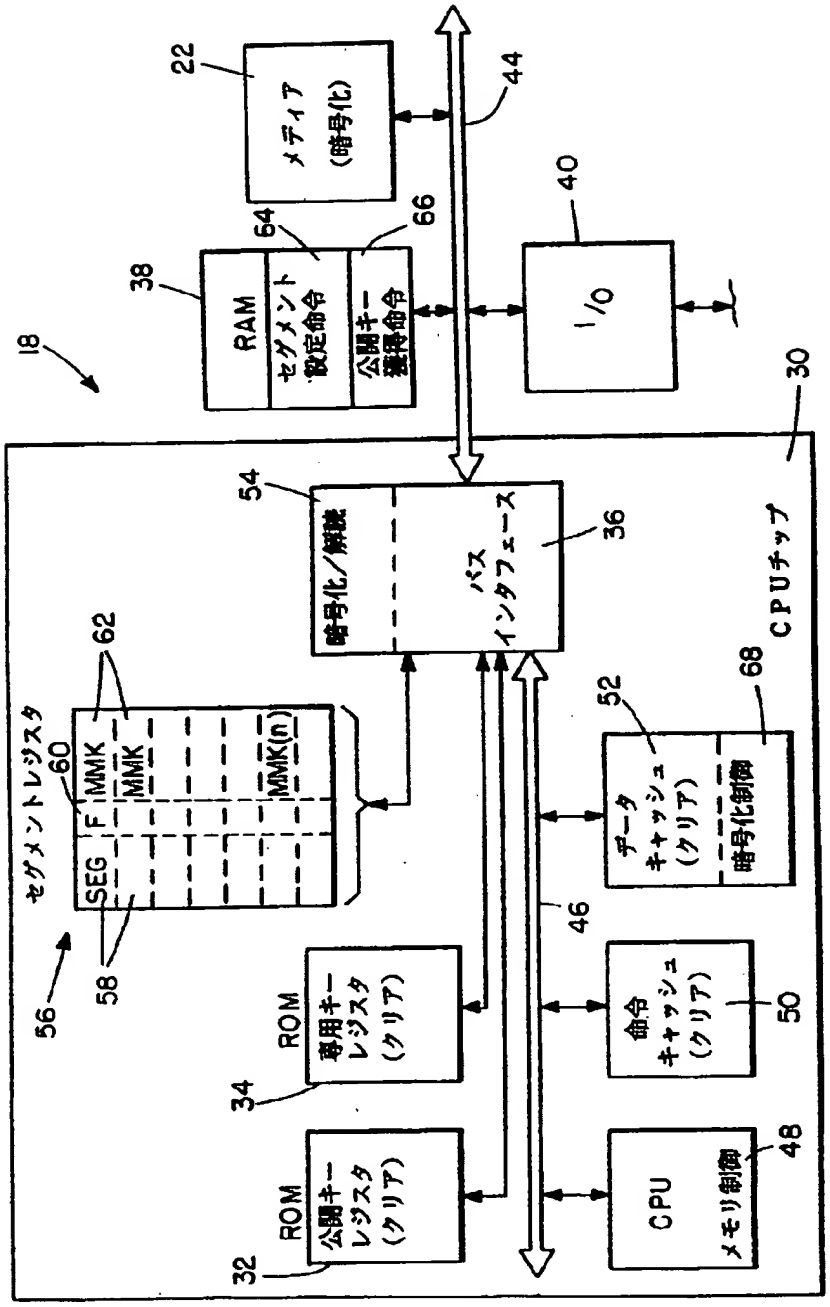
１０	メディア提供者
１２	公開キー
１４	専用キー
１６	MMK（メディアマスタキー）
１７	メディア
１８	遠隔プロセッサ
２０	二重通信チャネル
２２	暗号化メディア
３０	ＣＰＵ半導体チップ
３２	公開キーレジスタ
３４	専用キーレジスタ
３６	バスインタフェースモジュール
３８	ランダムアクセスメモリ（ＲＡＭ）
４０	Ｉ／Ｏポート
４８	ＣＰＵ
５０	命令キャッシュ
５２	データキャッシュ
５４	暗号化／解読モジュール
５６	セグメントレジスタ

６８　暗号化制御モジュール

【 図1 】



【 図2 】


22
メディア
(暗号化)
44
40
64
66
38
RAM
セグメント
設定命令
公開キー
登録命令
I/O
18
30
54
暗号化/解読
バス
インタフェース
36
CPUチップ
62
セグメントレジスタ
60
MMK
MMK
MMK(n)
F
SEG
52
68
データ
キャッシュ
(クリア)
暗号化制御
58
56
46
ROM
専用キー
レジスタ
(クリア)
34
命令
キャッシュ
(クリア)
50
ROM
公開キー
レジスタ
(クリア)
32
CPU
メモリ制御
48